Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene

Vendius, Trine Thygesen

Published in:
European Journal of Policing Studies

Publication date:
2015

Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene

Trine Thygesen Vendius[a]

Abstract

The European Cyber Crime Centre, EC3, established under the umbrella of Europol, started operations on January 1 2013. It is to act as the focal point in the fight against cybercrime in the European Union. Using a "shared, cross-community approach" the EC3 is concluding partnerships with member states, European agencies, international partners and the private sector. This article describes the coming about of EC3 and its efforts to address cybercrime. Furthermore, the article is an attempt to assess the growing role of the European law enforcement community on the European security scene, this not least in view of the EC3's mandate to conclude strategic agreements with a fairly high degree of autonomy.

Keywords: Europol; EC3; cybercrime; security, police agents; global governance

European Journal of Policing Studies, 3(2), 151-161
 | ISSN 2034-760X | December 2015

a Trine Thygesen Vendius is a post doc at the Faculty of Law, Copenhagen University (Corresp.: trine.thygesen.vendius@jur.ku.dk).
I wish to thank the anonymous referees for their comments on earlier drafts of this article.

1. Introduction

At the end of 2010, the European Commission announced its intention to establish a European Cyber Crime Centre (EC3) within the existing EU structure as part of the internal security strategy of the EU (The EU Internal Security Strategy in Action). Being the new flagship of Europol (the European Law Enforcement Agency), the EC3 is to act as the focal point in the fight against cybercrime in the European Union. Also the Stockholm Program: "An Open and Secure Europe Serving and Protecting Citizens"[1], emphasizes cyber-crime and network information security as priorities.

As for Europol, this agency became a reality with the Maastricht Treaty on February 17, 1992 in the aftermath of the end of the Cold War in order to deal with the so-called security deficit caused by new insecurities such as organized crime, illegal

1 The Stockholm Program is a five-year plan with guidelines for justice and home affairs of the Member States of the European Union for the years 2010-2014.

drugs, illegal immigration and terrorism (Buzan *et al.*, 1998; Bigo, 1996). In this context, the establishment of the EC3 as part of the EU Internal Security Strategy can be seen as a result of the growing "securitization" of cybercrime thus being articulated the new threat to European security.

This article seeks to address a rather underexplored question in relation to this development, namely the growing role of an organization such as the EC3 and its ability to enter into arrangements with third parties. In this respect, the growing role of the European law enforcement has not been addressed much in academia. As pointed out by Wessel (Wessel, 2008: 152), it is a fact that by the beginning of 2007, the EU had become part of some 90 international agreements as part of the European Security and Defense Policy (ESDP). However, when it comes to agencies involved in third pillar issues (Justice and Home Affairs), their external relations activities are rather underexplored (Ott, 2008: 518). This despite the fact that agencies increasingly seem to cooperate with third state's authorities, international programmes and organizations (Ott *et al.*, 2014: 88-89). In this respect, Europol is assumed to be one of the most significant actors in the European internal security regime (Mounier, 2009: 583). This is also the case, when observing the EC3, the European Cybercrime Center, being situated within Europol, the law enforcement agency of the European Union.

2. Defining Cybercrime

Unlike the case with Europol, there seems to be no major event that led to the establishment of the EC3. As pointed out by Buono (2012), it is difficult to indicate the precise date when the European Union decided to address the problem of cybercrime (Buono, 2012: 334).

On 23 November 2001 the Convention of cybercrime, also known as the Budapest Convention, was agreed upon, being the first international treaty addressing internet and computer crime. This convention, which entered into force in July 2004, seeks to harmonize national laws, improve investigative techniques and increase cooperation among nations and is so far the only binding international treaty on the subject which has been adopted to date. On a European level the Council Framework Decision 2005/222/JHA on attacks against information systems was adopted in 2005.

However, despite a growing focus on cybercrime in recent years – both in Europe and globally – there still lacks a single definition of cybercrime on a European level. In fact, it could be argued, that there are almost as many terms to describe cybercrime as there are cybercrimes and that a classification ought to distinguish between existing offenses committed in new ways and "true cybercrimes", e.g. offenses against computers and networks (Clough, 2010: 9-11). In this respect, such a definition can be found in the 2007 EU Commission's communication from 2007 dedicated to computer-related crimes has defined cybercrime as follows: "criminal acts committed using electronic communications, networks and information systems or against such networks and systems" (European Commission communication, 2007a).

In other words, the term "cybercrime" covers both new crimes specific to the Internet, e.g. attacks against information systems or phishing (fake bank websites to solicit passwords enabling access to victims' bank accounts) and so-called "Internet facilitated" crimes (or computer assisted crimes), e.g. crimes where computers used in an online environment are used as tools to commit more traditional crimes. These crimes are for example fraud, the dissemination of illegal content such as child sexual abuse material or incitements to violence on the Internet.

3. The Establishment of EC3 – a New, Innovative Step

The establishment of a European Cyber Crime Centre, EC3, was a first important step on a European level to address the growing threat from cybercrime. The EC3 became a reality shortly after the European Commission's proposal to establish a European Cyber Crime Center in 2010 as part of the EU Internal Security Strategy. The proposal was followed by a feasibility study funded under the ISEC Program (Internal Security Fund, the Prevention of and fight against crime) in the beginning of 2012, delivered by RAND Europe.[2] The RAND study served as the basis of the communication on a European Cyber Crime Centre re-commending the establishment of a European Cyber Crime Centre to be set up within Europol. Soon after, on 28 March 2012, the European Commission adopted a communication titled "Tackling crime in our Digital Age: Establishing a European Cyber Crime Centre". On July 1, 2012 the EC3 Implementation Team started its activities, and on January 1, 2013 the EC3 was live and operational with a staff of 64 people employed for the purpose of assisting EU Member States in the fight against cybercrime in the European Union.[3]

Less than a year after it became operational, the EC3 was already going strong. According to the first annual report of EC3, several analytical products had been produced focusing on the dark net and deep web, including bitcoins and the digital underground economy. In addition several knowledge products had been produced for the Member States' competent authorities, for instance the so-called ransom ware report and action plan, the strategic assessment on commercial exploitation of children online and the situation report on payment card fraud in the EU.

It should be mentioned, that also Interpol, the world's largest international police organization with 190 member countries, has set up a cybercrime centre, Interpol Global Complex for Innovation (IGCI), in Singapore. The centre started its operations in 2015 marking the transition of global policing into the digital age[4]. This step was eventually triggered as a result of Europol's innovative effort to tackle cybercrime in a more systematic manner, the latter being *first mover* in the area on a European level with the establishment of the EC3.

---

2 RAND Europe is an independent not-for-profit research institute whose mission is to help improve policy and decision-making through research and analysis.

3 According to (now former) Head of EC3, Troels Oerting, telephone interview, 1 November 2013.

4 INTERPOL's website, International gathering marks inauguration of INTERPOL Global Complex for Innovation, http://www.interpol.int/News-and-media/News/2015/N2015-039

On 25 September 2013 Europol and Interpol held their first joint Cybercrime Conference with the aim of enhancing international cooperation to tackle existing and future challenges in policing cyber space[5]. The borderless nature of cybercrime requires a global alliance in the fight against cybercrime. As stated in the first IOCTA report (Internet Organised Crime Threat Assessment, Executive Report 2014), law enforcement should concentrate on pro-active, intelligence-led approaches to combatting cybercrime through existing platforms such as the EC3 and Interpol's Global Complex for Innovation.

However, as the report also has stated, tackling cybercrime demands a different approach including new partners to be integrated into existing cooperation frameworks as it is the case with the EC3. This will be elaborated in the following.

4. A Shared, Cross-Community Approach: the Outreach Function

Initially it can be noted (when examining Europol's website), that the main functions of the EC3 are primarily focused on three areas: Cybercrimes committed by organized groups (particularly those generating large criminal profits such as online fraud); cybercrimes which cause serious harm to the victim (such as online child sexual exploitation) and finally, cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the European Union.6 As further stated on Europol's website, the EC3 serves as the central hub for criminal information and intelligence, supports Member States' operations and investigations by means of operational analysis, coordination and expertise and provides a variety of strategic analysis. Furthermore, the EC3 supports training and capacity building, provides highly specialized technical and digital forensic support and represents the EU law enforcement community in areas of common interest (R&D requirements, internet governance, and policy development). Finally, the EC3 establishes a so-called comprehensive outreach function connecting cybercrime related law enforcement authorities with the private sector, academia and other non-law enforcement partners. This outreach function together with the mandate to represent the EU law enforcement community of the EC3 will be further discussed below.

In this respect, according to a study from the European Parliament, we are now dealing with a "triangular diplomacy between states, companies and the inter-state system in the global regulation of the internet" (European Parliament, Study 2012). This has been further been explained by the EC3, as follows: "Since cyberspace and the internet's infrastructure are for the most part owned by the private sector, only a shared, cross-community approach will bring enduring results in the fight against cybercrime" (Frequently asked questions, MEMO/12/221). What here is interesting is that the EC3 is in charge of a so-called "outreach function". This outreach function both develops and maintains partnerships that can contribute to the EU Member States response to cybercrime in order to facilitate such cooperation,

[5] Europol's website, Europol-Interpol cybercrime conference steps up policing in cyberspace, https://www.europol.europa.eu/content/europol-interpol-cybercrime-conference-steps-policing-cyberspace

strengthen partnerships among various sectors, including the development of forums and projects and public private partnerships at national and international levels. The outreach function further includes the "proactive identification of new partners where required and cooperation with law enforcement agencies, EU institutions, international organizations, private industry, the public sector and academia".[6]

Thus, the EC3 concludes cooperation agreements with key actors that can contribute to the EU Member States response to cybercrime. In this respect, the term "Internet Governance" is to be understood as "the development and regulation of the Internet through shared principles, norms and programs" since the Internet "is governed through a multi-stakeholder approach, in a continuous and complex process".[7]

It could be argued, that in this way, the Internet is being framed as a sort of a "wild west" with reference to the borderless nature of the Internet and the lack of regulation in the field. As a consequence, the EC3 has provided itself with the task of a diplomatic role ensuring that common principles and norms are created through the deployment of a shared, cross-community approach when engaging in partnerships with Member States, private parties and third countries. In other words, what the EC3 itself has labeled its "outreach function". What further can be observed in this context is how the European law enforcement community gradually has gained the role of diplomatic entrepreneurs providing them with a high level of autonomy when it comes to concluding strategic partnerships in the area of cyber security.

A good example is Russia. Already half a year after the establishment of EC3 – in June 2013 – the Russian Federation officially visited EC3 for the first time in order to establish the basis for a future operational agreement. In this respect, Mr. Troels Oerting, (now former) Head of EC3, stated that the visit was "... an important step for the EU law enforcement community to engage in a more direct cooperation with the Russian Federation on cybercrime and cyber protection".[8]

In other words, we see that European Law Enforcement is entering in direct negotiations with third countries, in this case a superpower such as the Russian federation, outside the normal diplomatic framework of national state leaders. To put it into perspective: Simultaneously, Barack Obama, America's president was hosting his Chinese counterpart at an informal summit aimed at enhancing cooperation on cybersecurity.

---

6 Europol's website, outreach and cooperation, https://www.europol.europa.eu/ec3/outreach-and-cooperation

7 Europol's website, cyber community engagement, https://www.europol.europa.eu/ec3/cyber-community-engagement

8 Europol's website, First official visit of the Russian Federation to the European Cybercrime Centre, https://www.europol.europa.eu/latest_news/first-official-visit-russian-federation-european-cyber-crime-centre

5. The Growing Importance of Law Enforcement – a New World Order?

The situation described above underlines a development, which academia has labelled "a new global policing architecture" (Bowling & Sheptycki, 2012); describing also a situation where the practice of policing has been unhitched in various ways from the nation-state and resituated within "networks" of actors operating across national frontiers (Loader, 2002: 291).

And we see a new world order emerging, one which consists of global governance (Slaughter, 2005) and where various agents such as government officials, police investigators, judges etc. exchange information and cooperate across national borders to tackle crime, terrorism and international interactions. This complex global web of "government networks" challenges the notion of state sovereignty. But as Slaughter has put it, the state is not disappearing. On the contrary, it is disaggregating into separate, functionally distinct parts which are networking with their counterparts abroad, creating a dense web of relations that constitute a new trans-governmental order (Slaughter, 1997: 184). As Slaughter argues, this is not a collection of nation states that communicate through presidents, prime ministers, foreign ministers, the UN etc. On the contrary, police investigators, financial regulators, judges and legislators have taken over the role of government officials.

6. The Legal Basis for Concluding Agreements

As mentioned, the EC3 has been set up under the umbrella of Europol. Thus, the legal basis for the conclusion of agreements is to be found in the current 2009 Europol Council Decision, which authorizes Europol "to be able to conclude agreements and working arrangements with Union or Community institutions, bodies, offices and agencies in order to increase mutual effectiveness in combating serious forms of crime which come within the respective competence of both parties and to avoid the duplication of work". Under the current legal regime, strategic cooperation agreements generally provide for the exchange of all information (operational, strategic or technical) with the exception of personal data.

As stated in article 23(1) on "Relations with third States and organizations", Europol may establish and maintain cooperative relations with:

(a) third States;
(b) organisations such as:
    (i) international organisations and their subordinate bodies governed by public law;
    (ii) other bodies governed by public law which are set up by, or on the basis of, an agreement between two or more States; and
    (iii) the International Criminal Police Organisations (Interpol).

According to article 23(2), such agreements may concern the exchange of operational, strategic or technical information including personal data and classified information.

In principle Europol is accountable to the EU Member States through the Council members and the Europol Management Board. According to the wording of Article 218 TFEU, the power to conclude international agreements for the Union is conferred upon the Council (Ott *et al.*, 2014: 94). As pointed out by Busonic *et al.* (2013), the conclusion of Europol agreements with third countries, other EU bodies and international organizations illustrating Europol's unprecedented powers was made subject to control by the Council, and hence the director's autonomy on these issues was significantly circumscribed. Thus the director cannot start negotiations or sign an agreement without the Council's approval (Busonic *et al.*, 2013: 77). Enhanced control over Europol by the European Parliament and judicial control by the European Court of Justice is furthermore provided for in the 2009 Europol decision in order to ensure that Europol remains a fully accountable and transparent organization. As set out in Article 218 TFEU and depending on the kind of the international agreement, the Council would adopt the decision concluding the agreement after obtaining the consent of the European Parliament or after consulting it.

In this respect, it has been claimed that European integration has eroded the role of national parliaments in European decision-making to some extent; these agreements are hardly subject to democratic control neither through national parliaments nor the European Parliament, the latter having no real powers in deciding legislation affecting the powers of Europol. In fact, these agreements are barely known or debated outside the European Law Enforcement community. Which leaves European Law Enforcement with a rather high level of autonomy to act on the diplomatic arena on behalf of the EU Member States. In this respect Member States are quite concerned and need further clarifications as regards the future of Europol's relations with third countries (Discussion paper on Europol's agreements with third countries, 17, September 2013).

7. States Matter versus People Matter – the Proposal for a New Regulation on Europol

The legal framework for Europol is about to be changed in accordance with the Treaty of Lisbon – which provides for a new legal basis for Europol. On 27 March 2013, the Commission published a proposal for a 'Regulation on the European Police Office' (Europol). Article 88 and Article 87(2)(b) of the Treaty on the Functioning of the European Union are the legal bases for the proposal. The new regulation will eventually replace the current Europol decision. In the proposal for a Europol regulation, the establishment of a European Cyber Crime Centre is provided for in article 4(I) as part of Europol's tasks which include the ambition:

(l) to develop Union centres of specialised expertise for combating certain types of crime falling under Europol's objectives, in particular the European Cybercrime Centre.

In addition, the new Europol regulation is to provide for the following:

1. To establish Europol as a hub for information exchange between law enforcement authorities in the Member States

2. To set up a robust data protection regime.

What triggered the need for a Europol regulation was not least to impose the EU Member States the obligation to supply Europol with information. As stated in the Commission staff's working document accompanying the proposed regulation on Europol, the EU Member States do not provide Europol with all the necessary information to fight serious cross-border crime. As a result, Europol cannot be fully effective. As the common saying about Europol goes: "Europol is what the states make of it".

Meanwhile the EC3 seems to be a success in its own right. This is not least due to the (now former) Head of EC3, Troels Oerting, a trained police officer from Denmark. People working closely with him have described him as "the architect behind EC3"[9] and the absolute driving force of EC3, being both "extremely charismatic" and "very innovative and dynamic".[10] As a former Danish Europol liaison officer puts it: "One should not underestimate the importance of who is in charge. People matter".[11] In this respect Bowling & Sheptycki (2012) distinguish between eight archetypal global policing agents: The technician, the diplomat, the entrepreneur, the public relations' expert, the legal ace, the spy, the field-operator and the enforcer (Bowling & Sheptycki, 2012: 87-94). Oerting, who was nominated "Most Influential People in Security 2013" by the American "Security Magazine" in November 2013 is now employed by UK Bank Barclays, and in June 2015, Barclays and the EC3 signed a public/private sector information sharing agreement (SC Magazine, Further public/private cooperation as EC3 teams up with Barclays).

8. Conclusion

In this article I have sought to outline some observations related to the EC3, Europol's Cybercrime Centre, and its agreements with third parties as part of a growing trend, where European Law Enforcement increasingly has become an important player on the European security scene. In this respect I have elaborated on the so-called "outreach" function of the EC3 involving a "shared, cross-community approach" as part of what has been labelled a "triangular diplomacy between states, companies and the inter-state system". This outreach function connecting "cybercrime related law enforcement authorities

9 Interview with former head of Danish desk at Europol, December 5, 2013.

10 Author's conversations with representatives from Europol during visits to Europol, the EC3 and CEPOL, The European Police Academy as part of a 3 year PhD dissertation on Europol and Cybercrime (2011-2014).

11 Interview with former Danish Europol Liaison Officer, December 5, 2013.

with the private sector, academia and other non-law enforcement partners"[12] raises questions related to national sovereignty. Not least in an era of global governance where – as framed by Bowling & Sheptycki (2012) – "police power has begun to fly from its original nesting place within the nation-state-system" (Bowling & Sheptycki, 2012: 87-94).

Bibliography

Bigo, D. (1996). *Polices en reseaux, L'expérience européenne*. Presses de Sciences Po.

Bowling, B. & Sheptycki, J. (2012). *Global Policing*. Sage Publications.

Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A new set of rules and the establishment of the European Cybercrime Centre (EC3). *New Journal of European Criminal Law*, *3*(3-4), 332-343.

Busonic, M., Curtin, D. & Groenleer, M. (2013). Agency growth between autonomy and accountability: the European Police Office as a 'living institution'. In B. Rittberger & A. Wonka (Eds.), *Agency Governance in the EU*. Routledge, 70-87.

Buzan, B., Waever, O. & de Wilde, J. (1998). *Security. A New Framework For Analysis*. London: Lynne Rienner Publishers.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Discussion paper on Europol's agreements with third countries, Brussels 17 September 2013, Council of the Europen Union. Retrieved from: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013702%202013%20INIT, (accessed on 14 September 2015).

European Commission (2013). Commission Staff Working Document, impact assessment on adapting the European police Office's legal framework with the Lisbon Treaty, Accompanying the document, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Council Decisions 2009/371/JHA and 2005/681/JHA, Brussels, 27.3.2013, SWD(2013) 98 final, Part 1, pp. 8-14.

European Commission (2007a). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime, COM/2007/0267 final.

European Commission (2007b). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, "Towards a general policy on the fight against cybercrime", Brussels, 22.5.2007,COM(2007) 267 final.

European Commission (2012). Communication from the Commission to the Council and the European Parliament, "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre", Brussels, 28.3.2012, COM(2012) 140 final.

[12] Europol website, Combating Cybercrime in a Digital Age, https://www.europol.europa.eu/ec3

Convention on Cybercrime, Budapest, 23.XI.2001.

Council of Europe website, http://hub.coe.int/what-we-do/rule-of-law/cybercrime.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 069, 16/03/2005 p. 0067 – 0071.

EC3 First Year Report, 2013.

European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Study 2012, Fighting cybercrime and protecting privacy in the cloud.

Europol-Interpol (2013). Europol-Interpol cybercrime conference steps up policing in cyberspace, 25 September 2013. Retrieved from: https://www.europol.europa.eu/content/europol-interpol-cybercrime-conference-steps-policing-cyberspace (accessed on 14 January 2015).

Europol's website, Cyber Community engagement. Retrieved from: https://www.europol.europa.eu/ec3/cyber-community-engagement (accessed on 27 July 2015).

Europol's website, First official visit of the Russian Federation to the European Cyber Crime Centre. Retrieved from: https://www.europol.europa.eu/latest_news/first-official-visit-russian-federation-european-cybercrime-centre (accessed on 27 July 2015).

IOCTA, Internet Organised Crime Threat Assessment, Executive Report 2014.

INTERPOL's website, International gathering marks inauguration of INTERPOL Global Complex for Innovation, 13 April 2015. Retrieved from: http://www.interpol.int/News-and-media/News/2015/N2015-039 (accessed on 27 July 2015).

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An open, safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013) 1 final.

Loader, I. (2002). Governing European Policing: some problems and prospects. *Policing and Society, 12*(4), 291-305.

MEMO/12/221, Brussels, 28 March 2012, Frequently Asked Questions: the new European Cybercrime Centre. Retrieved from: http://europa.eu/rapid/press-release_MEMO-12-221_en.htm (accessed on 17 August 2015).

Mounier, G. (2002). Europol: A New Player in the EU External Policy Field? *Perspectives on European Politics and Society, 10*(4), 582-602.

Ott, A. (2002). EU Regulatory Agencies in EU External Relations: Trapped in a Legal Minefield Between European and External Law. *European Foreign Affairs Review, 13*, 515-540.

Ott, A., Vos, E. & Coman-Kund, F. (2014). European Agencies on the Global Scene. In M. Everson, C. Monda & E. Vos (Eds.), *European Agencies in between Institutions and Member States*. Wolters Kluwer, 87-117.

Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, Brussels, 27.3.2013, COM(2013) 173 final, 2013/0091 (COD).

SC Magazine, Further public/private cooperation as EC3 teams up with Barclays, Retrieved from: http://www.scmagazineuk.com/further-publicprivate-cooperation-as-ec3-teams-up-with-barclays/article/423594/ (accessed on 12 October 2015).

Slaughter, A.M. (2004). *A New World Order*. Princeton and Oxford: Princeton University Press.

Slaughter, A.M. (1997). The Real New World Order. *Foreign Affairs*, September/October, *76*(5), 183-197.

The Stockholm Program: An Open and Secure Europe Serving and Protecting Citizens, OJ C 115, 4.5.2010.

Wessel, R.A. (2008). The European Union as Party to International Agreements: Shared Competences, Mixed Responsibilities. In A. Dashwood & M. Maresceau (Eds.), *Law and Practice of EU External Relations – Salient Features of a Changing Landscape*. Cambridge University Press, 145-180.